7 TIPS FOR CRAFTING A STRONG PASSWORD

1. USE A STRONG PASSWORD

Strong passwords make it much harder for bad actors to break in. There are 3 ways hackers might try to breach your account. They may brute force your account, use password dumps found on the dark web, or send you a phishing email to trick you into handing over your credentials.

2. HAVE A LONG PASSWORD

Simply put, the longer a password is, the harder it is to crack. One thing security researchers have started recommending is to use a “passphrase” to make a long string of text easier to use. For example, “K33p0ut0fmy@cc0unt!!” is a 20 character password, but it is much easier to come up with and remember compared to a string of 20 random characters.

3. DON'T REUSE PASSWORDS

No matter how long and strong your password is, if you use it in multiple places it can leave you vulnerable. One thing hackers commonly do is to take a huge list of passwords leaked from previous breaches, and they try them on other sites and services.

4. DON'T INCLUDE PERSONAL INFORMATION

This is a fairly straightforward tip, but avoid including personal information in your password. These are things that could be easily guessed with some research or social engineering.

5. AVOID SEQUENTIAL CHARACTERS

You might think you’ve cracked the “strong password” code by running your finger across the keyboard, but in fact you’re probably in the majority. Just don’t do this. Many different versions of these are on the most popular password lists that even the most novice hacker will use to try to breach you.

6. USE A PASSWORD MANAGER

Password managers auto-generate and store strong passwords on your behalf. It’s incredibly useful and increases security while making it easier on you. These passwords are encrypted and kept in a centralized location, and you can access it with a master password.

7. USE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) adds an extra layer of security by requiring 2 (or more) methods of verification. A debit card is a good example of MFA. You’re combining something you have (the physical card) with something you know (your PIN).